REMARKS

The January 25, 2008 Office Action was based upon pending Claims 1, 5, 7, 8, 12-14, 17, and 20-24. Claims 1, 5, and 8 were amended by Applicant's response of March 25, 2008. The Advisory Action of May 1, 2008 indicates that Applicant's response was entered, but Claims 1, 5, 7, 8, 12-14, 17, and 20-24 are not allowed and remain rejected as in the January 25, 2008 Office Action. The Applicant notes that Claims 1, 5, 7, 8, 12, and 20-24 are amended by this paper to clearly point out and distinctly claim what the Applicant regards as the invention. Claim 1 for example is amended to recite "A method of transferring data over a computer network from a network server to a client computer system, the method comprising:

receiving a request by a requestor using a first client computer system for data from at least one network server storing data, at least some of the data stored by the network server being encrypted;

checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key;

if the requested data is encrypted with the encryption key, sending the encrypted data to the first client computer system ~~without an associated decryption key~~;

sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor;

if the requested data is unencrypted, automatically retrieving the encryption key associated with the requestor from the first client computer system and;

encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data; and

sending the encrypted data to the first client computer system ~~without the associated decryption key~~ wherein the client computer system uniquely retains a private key uniquely associated with the client computer system such that other client systems do not have access to the private key and wherein both the encryption key and the private key are needed for decryption of encrypted data"

Similar amendments are made to the other base Claims 5 and 8. Support for these amendments may be found for example at page 5, lines 19-25; page 6, lines 2-6; page 8, lines 15-17; page 9, lines 18-20, and page 10, line 23 of the subject application as filed.

In the Office Action, the Examiner objects to the Applicant's response of November 7, 2007 under 35 U.S.C. § 132(a) and rejects Claims 1, 5, and 8 under 35 U.S.C. § 112, first paragraph for entering new matter and failing to provide written description for the limitation of "without data indicative of an associated decryption key". The Applicant notes that the limitation of "data indicative of" is removed by Applicant's response of March 25, 2008. The Applicant further notes that the aspects of "without an associated decryption key" are removed by the present supplemental response. The Applicant believes that the amendments of this paper overcome the Examiner's remaining objections and rejections under 35 U.S.C. § 132(a) and 35 U.S.C. § 112, first paragraph and requests that the objections and rejections be withdrawn.

In the Office Action, the Examiner rejects Claims 1, 5, 8, 12, 13, 17, 20-22 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Hanna et al. (U.S. Patent No. 7,178,021) in view of Pond et al. (U.S. Patent No. 4,864,616) in view of Simmons et al. (U.S. Publication No. 2001/0039659) and further in view of Fan et al. (U.S. Patent No. 6,310,692). The Applicant has carefully reviewed the newly cited references and notes that Hanna et al. '021 describes methods and apparatus for utilizing a non-secure file server for storage and transmission of data in a secure manner among individual clients or groups of clients authorized access to the data. The encrypted data is stored on the file server and the encrypted first decryption key is stored on the file server and an access control list associated with the encrypted data." Col. 1, ll. 58-62. "In response to a request to access the encrypted data, the file server returns the encrypted data and at least the applicable encrypted first encryption key needed to decrypt the data" (Col. 2, ll. 4-6). Hanna et al. further describes "the encrypted data and the encrypted first decryption key K_{1d} along with a client or group identifier are forwarded over the network 10 by the client 12 C_a for receipt by the file server 14." (Col. 4, l. 67 — Col. 5, l. 3).

The Applicant thus notes that the primary reference cited by the Examiner, Hanna et al., describes a system supporting access to encrypted data to a plurality of clients who are a member of a defined group and, to facilitate this access, transmits encrypted data along with an encrypted decryption key. In contrast, the Applicant's claim includes sending encrypted data and/or

encrypting data, but where a private key needed for decryption of the data is unique to and maintained solely by a given client computer system. The Applicant further notes that Hanna et al. strongly teaches away from the Applicant's claimed invention by providing a system where multiple authorized users can have access to the same encrypted data by including decryption key information with encrypted data to which they have access, whereas the Applicant's invention limits access to encrypted data solely to a given client computer.

The Applicant has carefully reviewed the Pond et al. reference and notes that Pond et al. describe a method for cryptographically labeling electronically stored data as part of a security system for personal computers. Pond et al. describes encrypting data using two or more key streams and attaching a banner that is not encrypted but which announces that the associated file is protected. Pond et al. further describes that an Initialization Vector (IV) field of a label is filled with random bits. The random IV bits are used by the data ciphering processor to indicate a starting point for each key stream. In addition, the IV field may contain bits that indicate which of several reversible functions is to be used for encryption an decryption of the file and the direction in which the key streams are to be applied. Pond et al. further discloses that "much of the data necessary to decrypt an encrypted file is attached permanently to the file but is itself encrypted" (Col. 4, ll. 17-19). Pond et al. further describes "four bit flags of the Key Mix 36 are used to designate which of the optional key streams 16, 22, 24, 26 are to be used to encrypt or decrypt the file. At least one of the key stream flags of the key mix 36 **must be set** or else the file will not be encrypted and the label 30 will not exist." (Col. 6, ll. 28-34).

The Applicant notes that Simmons et al. '659 describes a transaction system for transporting media files from content provider sources to palm entertainment devices. The Applicant notes, however, that Simmons et al. fails to teach or suggest sending a message to a requester indicating that requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requester. Simmons et al. also fails to teach or suggest that if requested data is unencrypted, automatically retrieving an encryption key associated with the requester from the client computer system.

The Applicant notes that Fan et al. '692 describes a dynamic centralized printer resource management system to monitor printer resources and deliver warning messages to systems administrators, and users, and/or vendors when a printer resource falls below a predetermined

threshold. The Applicant agrees that Fan et al. does describe that, for example, thresholds for any monitored printer resource set by a second new printer attribute 264 can be changed by a system administrator as indicated by the Examiner at Column 4, lines 35-36, as indicated by the Examiner. However, Fan et al. fails to describe or suggest encryption or decryption protocols.

The Applicant thus respectfully notes that the combination of Hanna et al., Pond et al., Simmons et al., and Fan et al. fail to teach or suggest each and every element of the Applicant's claimed invention. The Applicant further believes that the ordinary artisan, at the time of invention, would have found the Applicant's invention to be obvious, considering the combined teachings of the art of record, the level of ordinary skill, and the nature of the problems addressed.

The Applicant thus believes that the Claims as currently amended are allowable and respectfully requests that the rejection of Claim 1 under 35 U.S.C. § 103(a) in light of these references be withdrawn. While Claims 5 and 8 recite different specific limitations, they are likewise believed patentable over the Hanna et al., the Pond et al., the Simmons et al., and the Fan et al. references as well as the other art of record for similar reasons to those previously indicated with respect to Claim 1. The Applicant thus believes that the remaining base claims 5 and 8 are also patentable and respectfully request that the rejection under 35 U.S.C. § 103(a) be withdrawn. The Applicant further believes that the remaining claims depending directly or indirectly from the corresponding base Claim 1, 5, or 8 properly further define the Applicant's claimed invention and are also patentable due at least in part to their dependence on the respective base claim.

The Examiner further rejects Claims 7, 14, and 23 under 35 U.S.C. § 103(a) as unpatentable over the combination Hanna et al, Pond et al., Simmons et al., and Eldridge et al. The Applicant notes that Eldridge et al. '721 describes methods and apparatus for updating password status for one or more servers in a client/server environment. Eldridge et al. further describes a key that may refer to any data or authentication information which is currently used by process to partake in an authentication protocol. For example, keys 308 may comprise a password itself, a one-way hash of a password, a public key corresponding to a private key derived from data including the password and others, however, Eldridge et al. fails to disclose or suggest the other limitations of the base claims and thus believes that Claims 7 and 14 are

patentable under the requirements of 35 U.S.C. § 103(a) in light of Hanna et al., Pond et al., Simmons et al., Fan et al., and Eldridge et al., due at least in part to their dependence on the respective base claim.

Co-Pending Applications of Assignee

Applicant wishes to draw the Examiner's attention to the following co-pending applications and issued patents of the present application's assignee.

Serial Number	Atty. Docket No.	Title	Filed
11/452594	MTIPAT.187C1	DATA SECURITY FOR DIGITAL DATA STORAGE	06/14/2006
11/521163	MTIPAT.187DV1	DATA SECURITY FOR DIGITAL DATA STORAGE	09/14/2006
09/277482	MTIPAT.075A	DATA SECURITY FOR DIGITAL DATA STORAGE	03/26/1999
10/962997	MTIPAT.075C1	DATA SECURITY FOR DIGITAL DATA STORAGE	10/12/2004
11/524097	MTIPAT.075C2	DATA SECURITY FOR DIGITAL DATA STORAGE	09/20/2006
09/277335	MTIPAT.076A	DATA SECURITY FOR DIGITAL DATA STORAGE	03/26/1999
11/503101	MTIPAT.076C1	DATA SECURITY FOR DIGITAL DATA STORAGE	08/11/2006

Copies of the patents, applications, and pending claims, including any office actions, Applicant's responses, and notices of allowance, are available through PAIR. However, if the Examiner so requests, Applicant will be happy to provide the Examiner with copies of any patents, applications, pending claims, office actions, allowances, or any other documents, at any time.

No Disclaimers or Disavowals

Although the present communication includes alterations to the claims, and characterizations of claim scope and referenced art, the Applicant is not conceding in this application that previously pending claims are not patentable over the cited references. Rather, any alterations or characterizations are being made to facilitate expeditious prosecution of this application. The Applicant reserves the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present

disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution. Accordingly, reviewers of this or any parent, child or related prosecution history shall not reasonably infer that the Applicant has made any disclaimers or disavowals of any subject matter supported by the present application.

SUMMARY

In view of the foregoing, the present application is believed to be in condition for allowance, and such allowance is respectfully requested. If further issues remain to be resolved, the Examiner is cordially invited to contact the undersigned such that any remaining issues may be promptly resolved.

Also, please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: June 12, 2008

By: _____

James W. Ausley
Registration No. 49,076
Agent of Record
Customer No. 20,995
(949) 760-0404

5458197